REMARKS

In response to the Office Action dated February 9, 2007, Applicant respectfully requests reconsideration. Claims 1-14 were previously pending in this application. Claims 1, 8, and 10 have been amended. New claims 15-17 have been added. No claims have been canceled. As a result, claims 1-17 are pending for examination with claims 1, 8, and 10 being independent. No new matter has been added.

I. Claim Rejections - 35 USC § 103

Claims 1-14 are rejected under 35 U.S.C. 103(a) as being allegedly obvious over Applicant's Admitted Prior Art (AAPA) in view of Published U.S. Patent Application No. 2003/223580 ("Snell"). Applicants respectfully disagree.

A. Claims 1-7, 9, and 15

Applicants' independent claim 1, as amended, recites a cyphering/decyphering method, by an integrated circuit, of a digital input code by means of several keys, comprising: dividing said code into several data blocks of same dimensions; applying to said blocks multiple turns of a cyphering or decyphering comprising submitting each block to at least one same non-linear transformation and of subsequently combining each block with a different key at each turn, and masking inputs and outputs of the non-linear transformation, upon execution of the method, by means of at least one first random number having the size of said code by combining, by an XOR-type function, the input and output blocks of the non-linear transformation with said at least one first random number, wherein the at least one first random number comprises a plurality of blocks of bits and wherein each block of bits is identical.

The combination of AAPA and Snell does not teach or suggest all the limitations of claim 1. Specifically, there is no disclosure in either the admitted prior art or in Snell regarding the specific contents of the random numbers. Claim 1 is limited to a random number "wherein the at least one first random number comprises a plurality of blocks of bits and wherein each block of bits is identical." There is no teaching to be found in either Snell or the admitted prior art of the exact contents of the random numbers. The Office Action asserts on page 4 that this limitation is taught in Applicants' admission of prior art, but the methods describe in the background of the instant application do not disclose any such requirement. Both the admitted prior art and Snell

simply disclose generating random numbers of a necessary length—Snell going one step further, requiring that the length of the random number equal that of the data to be ciphered—but neither reference discloses that the contents of the random number be limited to one in which all the blocks of bits are identical. Since claim 1 does recite the random number being comprised of a plurality of blocks of bits, and wherein each block of bits is identical, neither the admitted prior art nor Snell, alone or in combination, teaches all elements of claim 1, as required by MPEP §2143.

Therefore, claim 1 patentably distinguishes over the combination of the admitted prior art and Snell and is in condition for allowance. Claims 2-7, 9, and 15 depend from claim 1 and, based on their dependency, are allowable for at least the same reasons.

B. Claims 8-9 and 16

Applicants' independent claim 8, as amended, recites an integrated circuit for cyphering/decyphering by turn input data divided into blocks of same dimensions, comprising: means for generating at least one first random number of same size as the size of the blocks of the input data; and means for combining said random number with each block, at an input and at an output of a non-linear transformation implemented by the cyphering/decyphering, wherein the at least one first random number comprises a plurality of blocks of bits and wherein each block of bits is identical.

For reasons that should be clear from the above discussion in conjunction with claim 1, the admitted prior art in view of Snell does not teach or suggest all the limitations of claim 8. Specifically, the admitted prior art in view of Snell does not disclose a random number "wherein the at least one first random number comprises a plurality of blocks of bits and wherein each block of bits is identical." There is no teaching or disclosure in either the admitted prior art or in Snell regarding the specific content of the random number.

Therefore, claim 8 patentably distinguishes over the combination of the admitted prior art and Snell and is in condition for allowance. Claims 9 and 16 depend from claim 8 and, based on their dependency, are allowable for at least the same reasons.

C. Claims 10-14 and 17

Applicants' independent claim 10, as amended, recites a method comprising: dividing an

input into a plurality of data blocks of the same size; passing each data block of the plurality through a series of steps, each step applying a non-linear transformation and combining the result of the non-linear transformation with a key specific to the step to generate an output of the step; combining the output of each step, by an XOR-type function, with a random number having the same size as the output and being comprised of a repeated sequence of a value, wherein the random number comprises a plurality of blocks of bits and wherein each block of bits is identical.

For reasons that should be clear from the above discussion in conjunction with claim 1, the admitted prior art in view of Snell does not teach or suggest all the limitations of claim 10. Specifically, the admitted prior art in view of Snell does not disclose a random number "wherein the at least one first random number comprises a plurality of blocks of bits and wherein each block of bits is identical." There is no teaching or disclosure in either the admitted prior art or in Snell regarding the specific content of the random number.

Therefore, claim 10 patentably distinguishes over the combination of the admitted prior art and Snell and is in condition for allowance. Claims 11-14 and 17 depend from claim 10 and, based on their dependency, are allowable for at least the same reasons.

D. Claims 1-17 patentably distinguish over the combination.

In view of the foregoing, it is clear that no *prima facie* case of obviousness has been established, as there is no teaching or suggestion in the prior art of record that satisfies all the limitations of the pending claims. Therefore, it is respectfully requested that the rejection of claims 1-14 under §103(a) as purportedly being obvious over AAPA in view of Snell be withdrawn.

II. General Comments on Dependent Claims

Since each of the dependent claims depends from a base claim that is believed to be in condition for allowance, Applicants believe that it is unnecessary at this time to argue the allowability of each of the dependent claims individually. Applicants do not, however, necessarily concur with the interpretation of the dependent claims as set forth in the Office Action, nor do Applicants concur that the basis for the rejection of any of the dependent claims is

proper. Therefore, Applicants reserve the right to specifically address the patentability of the dependent claims in the future, if deemed necessary.

CONCLUSION

It is believed that all of the pending claims have been addressed. However, the absence of a reply to a specific rejection, issue, or comment set forth in the Office Action does not signify agreement with or concession of that rejection, issue or comment. In addition, because the arguments made above may not be exhaustive, there may be reasons for patentability of any or all pending claims (or other claims) that have not been expressed. Furthermore, nothing in this paper should be construed as an intent to concede any issue with regard to any claim, except as specifically stated in this paper, and the amendment of any claim does not necessarily signify any concession of unpatentability of the claim prior to its amendment.

In view of the foregoing amendments and remarks, this application should now be in condition for allowance. A notice to this effect is respectfully requested. If the Examiner believes, after this amendment, that the application is not in condition for allowance, the Examiner is requested to call the Applicants' representative at the telephone number indicated below to discuss any outstanding issues relating to the allowability of the application.

If this response is not considered timely filed and if a request for an extension of time is otherwise absent, Applicants hereby request any necessary extension of time. If there is a fee occasioned by this response, including an extension fee, that is not covered by an enclosed check, please charge any deficiency to Deposit Account No. 23/2825.

Respectfully submitted,

Dated: May 9, 2007

By: _____

Joseph Teja, Jr.
Registration No.: 45,157
WOLF, GREENFIELD & SACKS, P.C.
Federal Reserve Plaza
600 Atlantic Avenue
Boston, Massachusetts 02210-2206
(617) 646-8000